Requisição dos dados telemáticos na investigação criminal brasileira: Diagnóstico, fluxo de processo e cadeia de custódia apoiada pela tecnologia blockchain
Requirement of telematic data in Brazilian criminal investigation: Diagnosis, process flow and chain of custody supported by blockchain technology

Paulo Vitor Braga do Nascimento
Programa de Pós-graduação em Ciência da Informação
Universidade Federal de Santa Catarina, Brasil
MINTER - Policia Federal
E-mail: paulo.vbn@posgrad.ufsc.br
ORCID: 0000-0002-6611-3564

Gustavo Medeiros De Araújo
Programa de Pós-graduação em Ciência da Informação
Universidade Federal de Santa Catarina, Brasil
E-mail: gustavo.araujo@ufsc.br
ORCID: 0000-0003-0572-6997

RESUMO
A investigação criminal, após a revolução digital, passou a trabalhar com provas criminais das mais diversas fontes tecnológicas, necessitando, muitas vezes, de medidas legais para obtê-las junto às empresas de tecnologia e seu armazenamento de dados em nuvem. O objetivo geral da pesquisa é descrever o fluxo do processo de gestão dos dados telemáticos obtidos judicialmente na investigação criminal brasileira e os principais problemas encontrados baseados em avaliação diagnóstica na Polícia Federal do Brasil. A partir da identificação desses fluxos, analisar as principais causas e propor uma solução automatizada para o processo apoiada na tecnologia *blockchain*, com base na literatura correspondente. Neste trabalho, descrevemos algumas das principais dificuldades envolvidas no gerenciamento de provas digitais provenientes de intimações policiais, com foco no seu pré-processamento (aquisição, organização e armazenamento de dados) e na integridade da cadeia de

custódia. O trabalho foi respaldado por pesquisa diagnóstica institucional e pesquisa bibliográfica. Os resultados permitiram inferir algumas conclusões que corroboram o cenário prático. Não há uma rotina semelhante entre os diversos policiais, cada um em seu grupo de trabalho realizará a tarefa de forma análoga, mas não de forma padronizada. Uma arquitetura de plataforma web baseada na tecnologia *blockchain* foi proposta para melhorar o ciclo de vida e o uso de dados telemáticos de intimação no ambiente de investigação policial.

Palavras-chave: cadeia de custódia; evidência digital; *blockchain*; solicitações judiciais; investigação policial

ABSTRACT

After the digital revolution, criminal investigation began to work with criminal evidence from the most diverse technological sources. It often required legal measures to obtain them from technology companies and their data storage in the cloud. The general objective of the research is to describe the flow of the management process of the telematic data obtained judicially in the Brazilian criminal investigation and the main problems found based on diagnostic evaluation in the Federal Police of Brazil. From identifying these flows, analyze the leading causes and propose an automated solution for the process supported by blockchain technology based on the corresponding literature. In this work, we describe some of the main difficulties involved in managing digital evidence from police subpoenas, focusing on its pre-processing (data acquisition, organization, and storage) and the integrity of the chain of custody. The work was supported by institutional diagnostic research and bibliographical research. The results allowed inferring some conclusions that corroborate the practical scenario. There is no similar routine among the police officers; each in their work group will perform the task analogously but not in a standardized way. A web platform architecture based on blockchain technology was proposed to improve the life cycle and use telematic subpoena data in the police investigation environment.

Keywords: chain of custody; digital evidence; blockchain; law enforcement requests; police investigation

Como citar: Nascimento, P. V. B. do, & Araújo, G. M. D. (2023). Requisição dos dados telemáticos na investigação criminal brasileira: Diagnóstico, fluxo de processo e cadeia de custódia apoiada pela tecnologia blockchain. En E.B. Alvarez,

B. T. Alonso, P. C. Silveira (Eds.), Ciência da Informação e Ciências Policiais: Conexões e Experiências. *Advanced Notes in Information Science, volume 4* (pp. 251-287). Pro-Metrics: Tallinn, Estonia. DOI: 10.47909/anis.978-9916-9906-3-6.65.

INTRODUÇÃO

Segundo Zanini (2003), em seu intitulado artigo *A arte de comunicação telemática: a interatividade no ciberespaço*, a palavra telemática, foi cunhada na França em 1977, por Simon Nora e Alain Minc, significa a conectividade entre a tecnologia da informática e da telecomunicação e foi operacionalizada com as disponibilidades interfaciais das máquinas, criada em espaço multidimensional - o ciberespaço. Desta forma, o termo "telemática" resulta da junção das palavras telecomunicação (serviços de telefonia, fibra óptica, satélite, cabo, etc.) e informática (softwares, computadores, sistemas de redes, periféricos) e é qualquer sistema que transmite dados pela rede, seja em formato de texto, imagem ou som. Dados telemáticos, portanto, são todos e quaisquer arquivos oriundos deste universo digital criados pela união da informática e das telecomunicações.

A popularização da internet e de seu uso por dispositivos móveis já passou a fato cotidiano. Esse costume massificou o uso de redes sociais, comunicações instantâneas, aplicativos das mais variadas funções, troca de informações em áudio e vídeo quase em tempo real, transmissões de canais pessoais de vídeos, bem como a execução das mais variadas tarefas por meio remoto. Esse cenário, ainda agravado pela pandemia global, há tempos vem criando um extenso universo informacional. As crescentes informações oriundas do armazenamento de dados em nuvens,

bancos de dados com informações criminais, relatórios de informações financeiro-patrimoniais, entre outros, são fontes de informações importantes na investigação e na solução de crimes, além de ajudarem a compor evidências nos processos judiciais e orientar estratégias no combate à criminalidade.

Nesse cenário, os órgãos de segurança pública identificaram novas possibilidades de afastamento de sigilo, mediante ordem judicial, junto às empresas de tecnologia. A legislação brasileira permite avançar neste sentido, a partir do momento em que se pode afastar o sigilo de registros de acesso de aplicações de Internet, além da requisição de dados cadastrais e conteúdo armazenado. Naturalmente, passando a lidar com esse repositório investigativo como fonte de evidências criminais. Essa enxurrada tecnológica produz maciçamente milhares de dados diariamente implicando a necessidade de gerir e processar tais dados. A necessidade de aprimorar e até aprender a conviver com esse diverso e complexo volume de dados que exige recursos tecnológicos e metodologia adequada é fundamental para recuperar e transformar em informação útil ao contexto policial (Barth et al., 2007). Porém, o volume, complexidade e dispersão desses dados ainda dificultam o trabalho policial de investigação, exigindo sobretudo infraestrutura para trato com esses dados, além da garantia da autenticidade na cadeia de custódia da evidência.

Ainda precisa ser considerado, conforme esclarecem Martins e Vianna (2019), o paradigma cognitivo da informação, que considera os modelos mentais dos usuários, utilizando abordagens cognitivas, centradas no processo interpretativo do sujeito cognoscente sobre a informação que é produzida. A falta de padronização e metodologia técnica direciona cada investigador a gerir individualmente,

conforme sua cognição ou política local, a aquisição e o arquivamento digital, a cadeia de custódia da prova, dificultando, ainda, a integração das evidências digitais oriundas de múltiplas instâncias. Promove dificuldade para uma recuperação inteligente da informação ou uso de ferramentas de Inteligência Artificial (IA) e Mineração de Dados. Além disso, gera o risco do arquivamento digital inadequado e possível violação da cadeia de custódia da evidência criminal.

Neste ponto, a evidência digital poderia ser direcionada ao especialista forense, para processá-la e devolvê-la pronta ao investigador para análise; entretanto, a demanda para este tipo de trabalho é alta e exige sua célere análise. Isso resulta em excessiva demanda caso direcionada somente ao perito forense, sem mencionar que a aquisição dos dados ainda ficaria a cargo do investigador não perito. Abre-se, desta forma, uma nova frente de trabalho para o investigador não perito, a gestão direta daquela evidência digital e de sua cadeia de custódia. Na pesquisa realizada por Milagre e Segundo (2015, pp. 36-37) foram apontados relevantes pontos convergentes, como a ausência de um padrão para interconexão entre as empresas de tecnologia e as autoridades e investigadores, para manipulação dos dados das evidências digitais, o problema do armazenamento, os atores envolvidos e garantia da custódia, bem como outros desdobramentos.

Esse ambiente é semelhante ao trabalho com os arquivos gerados pelas medidas cautelares de quebra de sigilo telemático, atividade comum do investigador na qual a investigação criminal espera prosperar obtendo evidências para persecução criminal com o uso destas fontes tecnológicas. Com o aumento dessa demanda por requisições de dados, pela segurança pública, a maioria das grandes

empresas de tecnologia precisaram se especializar no atendimento destas requisições e atualmente utilizam um sistema conhecido como LERS (*Law Enforcement Request System*) ou Sistema de Solicitação de Aplicação da Lei, uma plataforma web em que agentes da lei podem enviar, com segurança, solicitações legais de dados, ver o status das solicitações enviadas e fazer o download dos dados telemáticos de interesse (Figura 1).

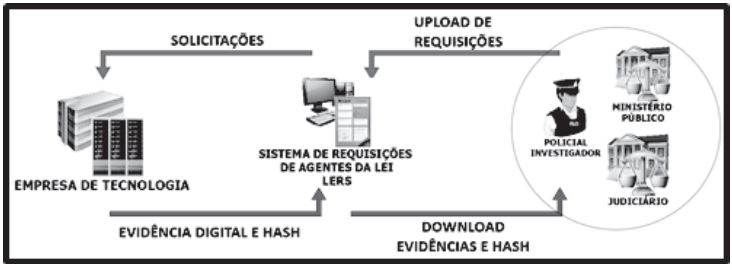

Figura 1. Plataforma de requisições das empresas de tecnologia (Fonte: elaboração dos autores, 2023).

Desta forma, autoridades podem realizar requisições e receber os dados extraídos de forma forense, diretamente. Destacamos, que neste processo normalmente não aparece a figura do perito forense. Fica claro que, na cadeia de custódia de evidências digitais, existe uma necessidade premente de manter a integridade das informações de uma maneira confiável e transparente. Geralmente, um valor *hash* de evidência digital é calculado e documentado com os dados adquiridos para provar que não foi alterado. No entanto, o valor de hash sozinho não prova que a evidência digital é a mesma de quando foi obtida, apenas que o conteúdo não foi modificado desde o momento em que o *hash* foi calculado (Burri et al., 2019).

Na imagem apresentada (Figura 1), as autoridades da lei por meio de seus representantes realizaram o procedente

de aquisição das evidências por meio de download diretamente da plataforma, momento em que o manuseio e a organização dos arquivos podem comprometer a cadeia de custódia. Com o desdobramento da nova frente de trabalho, as equipes de investigadores não peritos começaram a lidar, em seu cotidiano, com todo o processo envolvido na produção deste tipo de prova, realizando todo o procedimento de requisição e recepção (aquisição) dos dados junto às plataformas das empresas de tecnologia, seu armazenamento e manutenção da cadeia de custódia além da análise e produção de conhecimento (Figura 2).

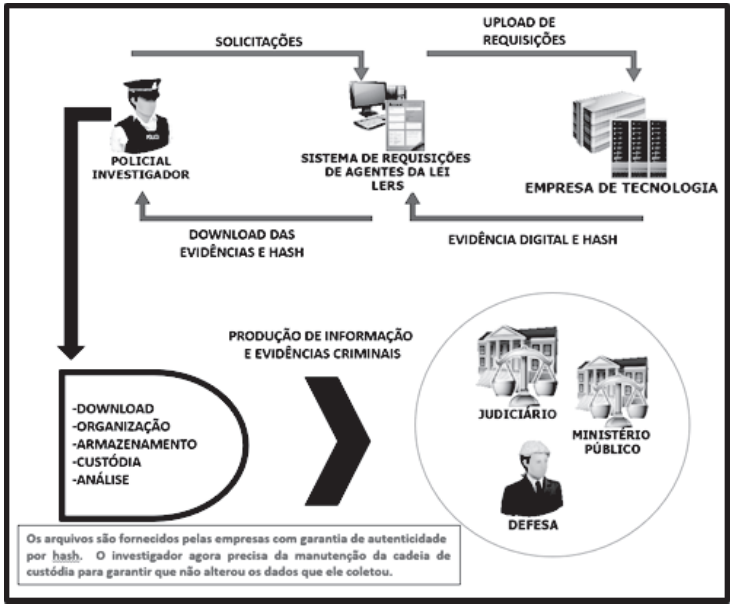

Figura 2. Rotina na obtenção de evidências digitais
(Fonte: elaboração dos autores, 2023).

A inexistência de ferramenta tecnológica ou automatização para aquisição, arquivamento digital, armazenamento e gestão do acesso a essas evidências pode prejudicar a

investigação criminal, devido ao procedimento sem padronização e manual (realizado pelo investigador), que cria um ambiente fragilizado ao processo legal e um problema a ser resolvido. A partir desse momento, a cadeia de custódia se mostra essencial para o processo de registro e preservação de detalhes de evidências digitais desde a coleta/armazenamento até a entrega ao Judiciário e demais personagens envolvidos na persecução criminal. Trazendo ao foco deste trabalho, sugere-se, no cenário da investigação policial, uma arquitetura de gestão dos dados telemáticos que aprimore esse ambiente e garanta que as evidências fornecidas permaneçam originais e autênticas e armazenadas de forma segura, apoiada na tecnologia *Blockchain* como mantenedora da cadeia de custódia. Essa tecnologia é conhecida por sua imutabilidade, integridade, disponibilidade, autenticidade e irretratabilidade de seus dados em rede, principais razões que a levam a interagir com a gestão de evidências digitais.

Apesar da proteção da cadeia de custódia por meio da tecnologia *Blockchain* encontrar diversos casos na literatura, este trabalho foi focado no entendimento do processo de obtenção dos dados oriundos de uma quebra de sigilo telemático em uma investigação policial e em uma avaliação diagnóstica, ambos realizados internamente na Polícia Federal Brasileira. O resultado apresentado aponta para grande possibilidade de aplicação da tecnologia *Blockchain* no cenário estudado. O principal problema na cadeia de custódia é a documentação e registro da interação com a evidência; quando esta é usada por múltiplas partes, já se associa um risco de adulteração. Por meio da tecnologia *Blockchain*, existe a possibilidade de se criar um livro-razão completo de todas as interações com a evidência de forma segura e inalterável. A elaboração de um sistema com a arquitetura proposta resolveria a questão do processo

manual e individual do investigador (própria expertise) na aquisição, no arquivamento digital, no armazenamento dos dados e na gestão da cadeia de custódia da evidência digital.

A INVESTIGAÇÃO CRIMINAL E OS DADOS DE FONTES TECNOLÓGICAS

A Ciência da Informação nasceu num cenário onde conseguia administrar, a geração e a organização da informação e, numa outra vertente, a transferência, preservação e recuperação da informação mediada pela tecnologia:

> A Ciência da Informação é a disciplina que investiga as propriedades e o comportamento informacional, as forças que governam os fluxos de informação, e os significados do processamento da informação, visando à acessibilidade e a usabilidade ótima. [...] está preocupada com o corpo de conhecimentos relacionados à origem, coleção, organização, armazenamento, recuperação, interpretação, transmissão, transformação. [...] uso de códigos para a transmissão eficiente da mensagem, bem como o estudo do processamento e de técnicas aplicadas aos computadores e seus sistemas de programação (Borko, 1968, pp. 1-2).

A necessidade de gerir e organizar a informação de forma metódica e científica data de muito tempo, e há muito já se planejava executar tais tarefas com auxílio de tecnologia computacional. Ainda conforme o entendimento de Saracevic (1996 *apud* Mooers, 1951), o futuro uso do *Big Data* poderia ser estruturado pela Ciência da Informação,

sendo até hoje peça-chave na recuperação de informação por meios tecnológicos.

> Considerando o problema da informação definido, isto é, a explosão informacional, a recuperação da informação tornou-se uma solução bem-preparada encontrada pela CI e em processo de desenvolvimento até hoje. Como toda solução suscita seus próprios e específicos problemas, assim também a recuperação da informação" e esses problemas estão contidos na concepção proposta por Mooers:
> a) como descreve intelectualmente a informação /
> b) como especificar intelectualmente a busca? /
> c) que sistemas, técnicas ou máquinas devem ser empregados? (Saracevic, 1996, p. 44)

A Ciência da Informação exerce papel fundamental, pois seus estudiosos começaram com uma vantagem competitiva em relação ao *Big Data*: sabiam como armazenar, gerenciar e processar dados; e entendiam a complexidade das estruturas de dados muito cedo na história da Ciência da Informação. Conheciam, ainda, os desafios associados à infraestrutura necessária para lidar com o volume de dados que está sendo gerado hoje (Agarwal, & Dhar, 2014). A Ciência da Informação pode ser considerada como uma ciência multi e interdisciplinar, característica-chave para lidar com um universo informacional tão diverso em sua estrutura e conteúdo como é o caso de datasets complexos. Como assevera Saracevic (1995), a Ciência da Informação possui três características fundamentais: sua interdisciplinaridade, sua inexorável conexão com a tecnologia da informação e ainda uma ativa participação na evolução da sociedade da informação.

Os dados são considerados o novo petróleo da era digital. Embora não exista uma universalização do conceito de *Big Data*, sobretudo no meio acadêmico, por se tratar de um termo relativamente novo (Souza, 2018). O crescimento e a integração de grandes volumes de dados digitais – vulgarmente chamado *Big Data* – têm sido utilizados para tomada de decisão em diferentes áreas. Obviamente o serviço de segurança pública e o sistema de investigação incluem o rol dos ramos onde a presença do *big data* é relevante, principalmente com as enormes quantidades de informações oriundas de fontes tecnológicas disponíveis no cotidiano (redes sociais, comunicações instantâneas, aplicativos diversos, transmissão de áudio e vídeo em tempo real) fato que vem se consolidando há alguns anos com o uso de medidas cautelares de quebra de sigilo de dados telemáticos para obtenção de provas no âmbito da persecução criminal. Neste ponto, para o desenvolvimento da investigação, o Código de Processo Penal Brasileiro (1941) permite a representação por medidas judiciais para obtenção de dados telemáticos junto a empresas de tecnologia. Cenário que traz enormes quantidades de informações digitais oriundas de fontes tecnológicas.

Assim, não faltam exemplos para se observar o crescente volume de tráfego de informações ao redor do mundo, implicando um aumento cada vez maior de arquivos oriundos das fontes tecnológicas. Este novo mundo informacional vem ampliar o horizonte da investigação, quando nos deparamos com a existência das demais fontes de dados tradicionais, como registros policiais, banco de dados de registros civis e materiais apreendidos em operações policiais (Saisse, 2017). Em função dessa nova realidade, surge a necessidade de repensar nos métodos de gestão, organização, tratamento e armazenamento desses arquivos para

uma recuperação inteligente da informação em uma investigação policial. Neste ambiente digital tão vasto e de rápida evolução, também surgiram as tecnologias disruptivas, termo que descreve uma inovação tecnológica, como por exemplo a tecnologia *Blockchain* e o armazenamento digital distribuído em nuvem.

Neste ambiente as etapas de coleta e armazenamento inicial dos dados a serem utilizados são de fundamental importância. E não deve ser tratada de forma individual e pessoal nas diversas instâncias investigativas, ao contrário, deveria ser trabalhada de forma padronizada, para garantir a autenticidade dos dados, condição primaria de uma cadeia de custódia de uma evidência criminal.

GESTÂO DOS DADOS TELEMÁTICOS E O SEU CICLO DE VIDA

Na investigação durante a realização de diligências extraordinárias, como a representada pela medida cautelar de quebra de sigilo telemático, após fundamentação dos pedidos e representação da autoridade policial e deferimento pela justiça,

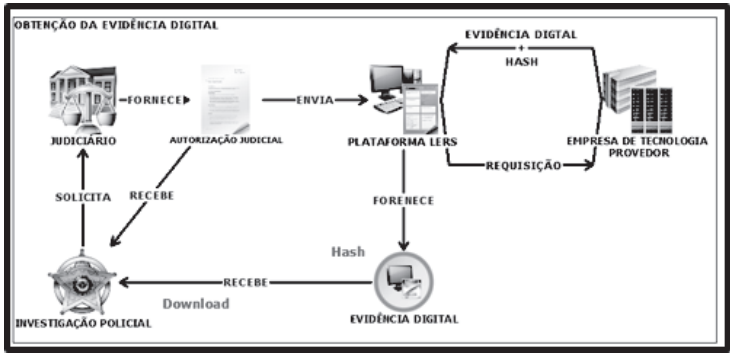

Figura 3. Ciclo de obtenção de evidência digital (Fonte: elaboração dos autores, 2023).

o investigador tem o instrumento necessário, uma ordem judicial, para solicitar junto aos provedores e empresas de tecnologia os dados convenientes ao processo investigativo, conforme autorizado explicitamente. Momento de aquisição dos dados, onde o investigador precisa interagir com a plataforma de requisições das empresas de tecnologia para o envio da ordem judicial (Figura 3).

Ainda na de aquisição, novamente o investigador interage com plataforma de requisições para o *download* dos dados solicitados, normalmente entregues de forma forense, com *hash*, ao investigador. A partir deste momento, com a realização deste *download* de arquivos inicia-se a etapa de manuseio dos dados, onde a cadeia de custódia da evidência digital conta com a participação direta do investigador, processo fragilizado pela interação humana. E conforme identificado na pesquisa diagnóstica, as maiores dificuldades seriam armazenamento, organização e velocidade da rede (Figura 4).

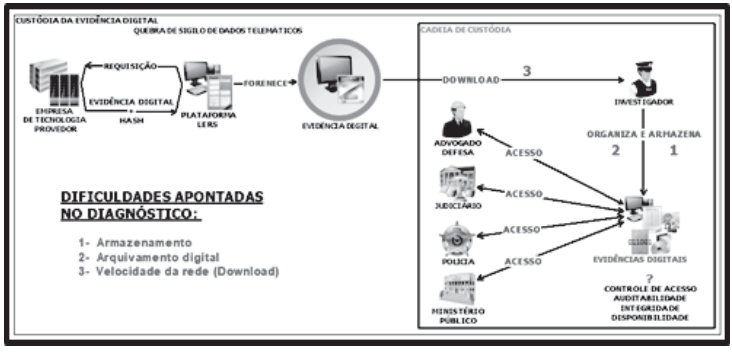

Figura 4. Ciclo de vida da evidência digital fragilizado (Fonte: elaboração dos autores, 2023).

Neste ambiente, o investigador e sua cognição, a interação humana, respondem diretamente pelo ciclo de vida da evidência e sua cadeia de custódia. Têm o controle e a personalização

da coleta, arquivamento digital preliminar e armazenamento dos dados fornecidos, abrindo possiblidade de falhas ou comprometimento da prova criminal nos trabalhos investigativos. Além de controle precário das interações e manuseio das evidências na cadeia de custódia.

BLOCKCHAIN E CADEIA DE CUSTÓDIA

A cadeia de custódia documental pode ser entendida como o ambiente no qual perpassa o ciclo de vida dos documentos. Em outras palavras, ela define quem é o responsável por aplicar os princípios e as funções arquivísticas à documentação. (Flores, 2016). Um dos maiores desafios na cadeia de custódia de arquivos digitais é manter a integridade dos dados. Uma falha de segurança no manuseio dessas evidências põe em risco todo o processo criminal. De acordo com Bonomi *et al*. (2018), a cadeia de custódia é o processo de validação de como qualquer tipo de evidência foi recolhida, rastreada e protegida no caminho até o judiciário. A evidência digital é parte integrante do processo de investigação. Assim, no processo judicial também, as evidências desempenham um importante papel. A principal razão que nos leva a interagir com a tecnologia Blockchain é possibilidade de se criar um livro-razão completo de todas estas interações com a evidência digital de forma segura e inalterável.

Em uma definição mais simples, *Blockchain* é um registro descentralizado e distribuído de informações que é controlado e atualizado por uma comunidade de usuários. Não existe uma entidade ou pessoa central que controle o registro. Na origem da *Blockchain,* está o protocolo do Bitcoin, proposto por Satoshi Nakamoto (Nakamoto 2008), que entrou em operação em 2009. O artigo seminal propõe uma rede puramente *peer-to-peer* (arquitetura de redes de computadores onde cada um dos pontos ou nós da rede,

funcionam tanto como cliente quanto como servidor) de dinheiro eletrônico que permitiria que pagamentos *online* fossem enviados diretamente de uma parte para outra sem passar por uma instituição financeira, no sistema de rede descentralizado e distribuído. As transações propostas por clientes (nós), são recebidas por servidores (mineradores), que irão decidir, através de um protocolo de consenso bizantino (um protocolo de consenso que tolera falhas do tipo bizantina) à base de desafios criptográficos, sobre a ordem em que as transações serão realizadas e armazenadas permanentemente numa corrente de blocos (*Blockchain*), replicada em cada servidor.

É de extrema importância garantir integridade, autenticidade e auditoria de evidências digitais à medida que se move em diferentes níveis de hierarquia, ou seja, dos investigadores que obtém a prova, até as autoridades do judiciário, Ministério Público e Defesa, responsáveis por lidar com a investigação e com as instancias de defesa do acusado. O principal problema na cadeia de custódia é a documentação e registro da interação com a evidência, quando a evidência é usada por múltiplas partes já se associa um risco de adulteração. A capacidade da tecnologia *Blockchain* de se dividir em diversos registros que permitem um abrangente rastreamento das informações atreladas àqueles registros desde sua origem, abre uma monumental possibilidade para a comunidade forense, permitindo o registro de movimentação de uma evidência em toda a sua cadeia de custódia, do começo ao fim. Basicamente, uma informação distribuída que mantém uma estrutura a prova de adulteração incessantemente crescente em seus diversos blocos de transações individuais, implementando um livro-razão descentralizado e totalmente replicado em uma rede *peer-to-peer* (Gopalan, 2019).

METODOLOGIA

A seção apresenta o percurso metodológico para a realização da pesquisa e alcance dos objetivos previamente estabelecidos. O trabalho realizado foi organizado em algumas etapas descritas a seguir:

- Mapeamento bibliográfico e pesquisa sobre estudos aplicados ao arquivamento digital, armazenamento e custódia das evidências digitais apoiados na tecnologia *Blockchain* (tecnologia que possibilita manutenção da integridade, autenticidade e auditoria de seus dados). Para tanto, foram selecionadas as bases de dados que se mais se relacionavam com o assunto. Foram consultados e selecionados trabalhos através das bases de publicações científicas *ScienceDirect*, *Web of Science*, *Scopus* e *IEEE Xplore*. A seleção das bases se sustentou na relevância de cada uma delas no meio acadêmico e científico e na área de domínio de suas coleções. Inicialmente, foram escolhidos termos relacionados à tecnologia *Blockchain* e armazenamento e o envolvimento na investigação policial. Foram pesquisados os termos combinados nos títulos dos artigos: *"digital forensics"*, *"digital evidence"*, *"Blockchain"*, *"chain of custody"*, *"law enforcement"*. O período escolhido para a pesquisa foi a partir do ano de 2012, apesar de a primeira publicação a respeito do uso de *Blockchain* ser anterior (Nakamoto, 2009), pois entendemos que o uso do protocolo se difundiu e amadureceu a partir do ano de 2012;
- Esquematização do modelo do ciclo de vida das evidências digitais, dados oriundos de medidas cautelares de quebra de sigilo de dados telemáticos usados na investigação. Realizou-se uma representação gráfica baseado no fluxo de trabalho e das atividades relacionadas, com

apoio do software Bizagi (modelagem do processo);

- Avaliação diagnóstica por meio de questionário aplicado dentro da instituição Polícia Federal, no nicho de servidores que lidam com a temática de investigação com a quebra de sigilo telemático. Os convidados responderam a um questionário objetivo, com seis perguntas e com 3 a 5 opções de respostas, sendo cerca de 50 servidores que tiveram ou têm atuação com o manuseio de dados telemáticos. As questões foram elaboradas e respondidas por meio da plataforma Google, na ferramenta Google Forms. Esta avaliação preliminar não esgota o assunto e muito menos elimina um diagnóstico mais profundo; no entanto, as repostas foram bastante esclarecedoras, corroborando o direcionamento desta pesquisa;
- E por fim, baseado nos resultados da pesquisa, a sugestão de uma proposta de arquitetura de sistema apoiada pela tecnologia *Blockchain*, para gestão dos dados telemáticos na investigação criminal.

TRABALHOS RELACIONADOS

Depois do mapeamento da literatura relacionada, identificamos diversas propostas com características diferentes de utilização da tecnologia *Blockchain* para apoio a cadeia de custódia de evidências digitais. Todas visando fornecer integridade, preservação, transparência e resistência à adulteração das evidências, em todo o ciclo de vida, da coleta de evidências até a preservação e no manuseio por várias partes interessadas ao mesmo tempo. Nenhum dos trabalhos abordou a aquisição de evidências digitais por meio das plataformas de requisições de autoridades da lei das empresas de tecnologia. Assim, sugerimos um modelo de arquitetura para atender esta característica.

Tabela 1. Resumo dos trabalhos mapeados na literatura (Fonte: elaboração dos autores, 2023).

	Título do trabalho	Proposta	Tipo de blockchain	Referência
1	*B-CoC: A Blockchain -Based Chain of Custody for Evidence Management in Digital Forensics*	O trabalho apresenta uma arquitetura de cadeia de custódia baseada em *Blockchain* (B-CoC) que visa garantir a integridade da auditoria da coleta de evidências digitais e a rastreabilidade das partes interessadas. Desenvolveram um protótipo de B-CoC baseado em *Ethereum* e avaliaram o seu desempenho. A escolha foi motivada pela autenticação requisito do processo de cadeia de custódia (CoC), que não permite que partes não autorizadas e não confiáveis gerenciem evidências digitais e, portanto, estejam na rede.	Privada	Bonomi, S. *et al.*
2	*Blockchain-based Chain of Custody - Towards Real-time Tamper-proof Evidence Management*	O artigo propõe uma cadeia de custódia segura por meio de um framework baseado em *Blockchain*, para armazenar os metadados da evidência enquanto a evidência é armazenada em um meio de armazenamento. A estrutura é construída em cima de uma derivação da rede *Ethereum*, oferecendo uma *Blockchain* hibrida.	Híbrida	Ahmad, L. *et al.*

3	*Block-DEF: A secure digital evidence framework using Blockchain*	A pesquisa apresenta uma estrutura de evidência digital chamada *Block-DEF*, suportada em *Blockchain* para apoiar a coleta, armazenamento, verificação e recuperação de evidências. Seu design armazena as informações de evidências na *Blockchain* e preserva as evidências em uma plataforma de armazenamento confiável. E usam dois esquemas de assinatura múltipla para envio e recuperação de evidências, de modo a garantir a rastreabilidade.	Consórcio ou Privada	Tian, Z. H. *et al.*
4	*Chronological independently verifiable electronic chain of custody ledger using Blockchain technology*	O artigo propõe um livro-razão (*ledger*), cronológico, independente e verificável usando a tecnologia *Blockchain*, hospedada por uma entidade confiável e acessada para verificar os detalhes da cadeia de custódia. As informações confidenciais não são armazenadas nos registros da *Blockchain*, são enviadas periodicamente para um *Blockchain* público, para provar que o próprio *ledger* não foi modificado. Garantindo a integridade por sua descentralização e pela estrutura de um *ledger* seguro. Nem todos os blocos são enviados para uma *Blockchain* pública que permite diferentes níveis de verificação.	Híbrida	Burri, X. *et al.*

	Título do trabalho	Proposta	Tipo de blockchain	Referência
5	Digital forensics using Blockchain	A pesquisa propõe o uso de *Blockchain* para garantir a integridade do sistema e preservar a integridade das evidências para que possam ser aceitas judicialmente. Afirma que os principais requisitos de um processo de CoC são: a integridade e a rastreabilidade. Aproveitando esses recursos, o autor definiu uma arquitetura capaz de suportar o processo de CoC criando uma *Blockchain* pública e permissionada para impor um contrato inteligente que acompanhe as mudanças de posse ao longo do ciclo de vida da prova.	Consórcio	Gopalan, S. H. *et al.*
6	*Digital Forensics: Maintaining Chain of Custody Using Blockchain*	O trabalho propôs um sistema baseado em *Blockchain* usando *Hyperledger*, no qual as evidências estão sendo rastreadas, transferidas, registradas e atualizadas com segurança, mantendo as evidências imutáveis e íntegras na cadeia de custódia descentralizada do aplicativo. O caso preservado, é distribuído legalmente e apresentado no tribunal.	Consórcio	Chopade, M. *et al.*

7	*Distilling Blockchain requirements for digital investigation platforms*	A pesquisa propõe metodologias e frameworks para a aplicação de *Blockchain* para auxiliar investigações de segurança cibernética. O serviço *Blockchain* é executado em infraestruturas críticas como uma medida de serviço proativo para registrar ações na resposta e investigação de incidentes. As atividades de execução de qualquer ação na plataforma de gerenciamento de resposta a incidentes, de uma maneira cronológica e funcionado como um sistema eletrônico verificável independente. A estrutura serve para garantir a integridade de ações investigativas forenses digitais e os dados de evidências.	Privada	Olukoya, O.
8	*Forensic-chain: Blockchain based digital forensics chain of custody with PoC in Hyperledger Composer*	Esta pesquisa propõe uma cadeia de custódia forense digital baseada em *Blockchain*, trazendo integridade e resistência à adulteração para a cadeia de custódia forense digital. O modelo proposto foi construído no Hyper*ledger* Composer, uma *Blockchain* permissionada de consórcio ou privada (onde uma única organização controla). Assim as informações sobre a evidência são confinadas apenas aos participantes que fazem parte do *Blockchain*, autorizado por administradores pertencentes a organização do consórcio.	Consórcio ou Privada	Lone, A.H *et al.*

	Título do trabalho	Proposta	Tipo de blockchain	Referência
9	*LEChain: A Blockchain -based lawful evidence management scheme for digital forensics*	Propõe uma arquitetura chamada de *LEChain*, um esquema de gerenciamento de evidências legais baseado em *Blockchain* para supervisionar todo o fluxo de evidências e todos os dados do Judiciário (por exemplo, votos e resultados de julgamentos), estendendo-se desde a coleta de provas e acesso durante a investigação policial até a votação do júri nos julgamentos.	Consórcio	Li, M. *et al.*
10	*MF-Ledger: Blockchain Hyperledger Sawtooth-Enabled Novel and Secure Multimedia Chain of Custody Forensic Investigation Architecture*	O trabalho apresenta a chamada MF-*Ledger* uma proposta, baseada na *Blockchain Hyperledger*, de arquitetura de investigação forense digital nova, segura e eficiente, onde as partes interessadas participantes criam uma rede privada para troca e consenso das diferentes atividades de investigação antes de destas serem armazenadas no livro-razão da *Blockchain*, por meio de uso de contratos inteligentes. A solução proposta oferece integridade de informações, prevenção e mecanismo de preservação robustos para armazenar de forma permanente e imutável as evidências (cadeia de custódia) em um livro-razão criptografado com permissão.	Privada	Khan, A. *et al.*

11	*Smart contracts applied to a functional architecture for storage and maintenance of digital chain of custody using Blockchain*	A pesquisa apresenta um sistema direcionado aos participantes envolvidos na cadeia de custódia das evidências legais digitais baseado em *Blockchain* para garantir os requisitos legais. A plataforma permite, além do necessário armazenamento de provas digitais, a consulta por operadores do direito, os responsáveis pela execução processo, como advogados, juízes e promotores. Auxiliando no armazenamento das evidências digitais coletadas por especialistas e na adoção de mecanismos padronizados que permitem que outros operadores de aplicação da lei acessem, mantenham e usem a cadeia de custódia de evidências digitais na forma da lei, dentro do total garantia de integridade e confiabilidade.	Híbrida	Petroni, C. A. *et al.*
12	*Storing and Securing the Digital Evidence in the Process of Digital Forensics through Blockchain Technology*	O trabalho ressalta a importância que a evidência tem no caso investigado, desempenhando papel vital no julgamento. Propõem, então, a utilização da tecnologia *Blockchain*, que possui propriedades de alta segurança. Na tecnologia, um registro na rede possui um *hash* com o registro anterior, gerando um encadeamento criptografado, o que garante a imutabilidade no livro-razão e, assim, nas evidências digitais.	Privada	Anne *et al.*

MODELAGEM DO PROCESSO - CICLO DE VIDA DOS DADOS

A modelagem de processos de negócios é um mecanismo de representação gráfica que ajuda a melhorar a compreensão de um contexto, as etapas realizadas, as validações e regras de negócios que fazem parte de seu universo (Pastrana-Pardo *et al.*, 2022). Foi elaborada uma representação gráfica com o fito de esquematizar o modelo do ciclo de vida dos dados oriundos de medidas cautelares de quebra de sigilo de dados telemáticos usados na investigação. Desta forma, foi feita uma modelagem do processo, uma representação gráfica do fluxo de trabalho e das atividades, com apoio do software *Bizagi*.

Utilizou-se o *Business Process Model and Notation* – BPMN, notação da metodologia de gerenciamento de processos de negócio que trata de uma série de ícones padrões para o desenho de processos, o que facilita o entendimento do usuário e a representação gráfica do fluxo de trabalho e das atividades. Os fluxos gerais dos processos de aquisição e manuseio dos dados são apresentados na figura abaixo (Figura 5) e nas seguintes (Figura 6 e 7), nas quais são detalhadas as duas etapas separadamente.

DIAGNÓSTICO

A etapa de Diagnóstico foi realizada através de uma avaliação diagnóstica por meio de um questionário aplicado dentro da Instituição Polícia Federal Brasileira, no nicho de servidores que lidam com a temática de investigação com o uso de evidências digitais (quebra de sigilo telemático). Os convidados responderam a um questionário objetivo, com seis perguntas e com 3 a 5 opções de respostas, sendo cerca de 50 servidores que tiveram ou têm atuação com o manuseio de dados

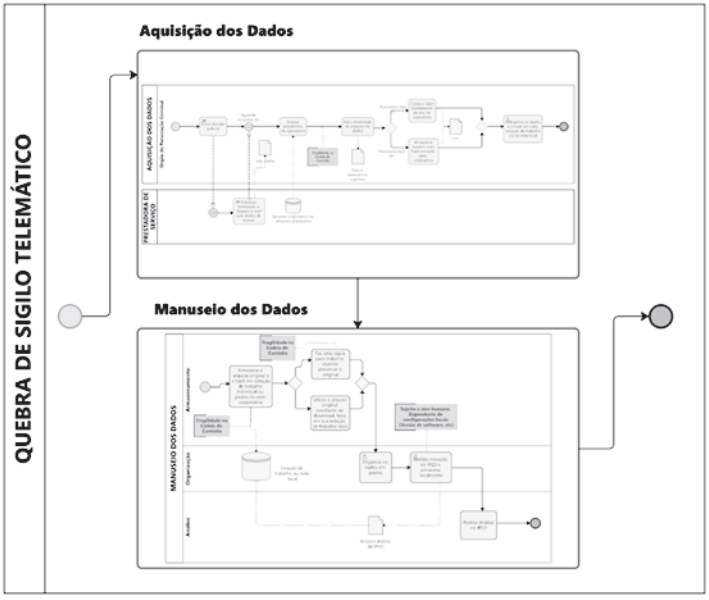

Figura 5. Modelagem quebra de sigilo - Gera (Fonte: elaboração dos autores, 2023).

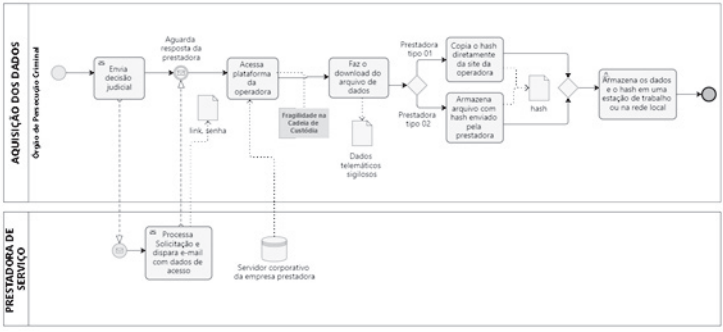

Figura 6. Modelagem - Aquisição de dados (Fonte: elaboração dos autores, 2023).

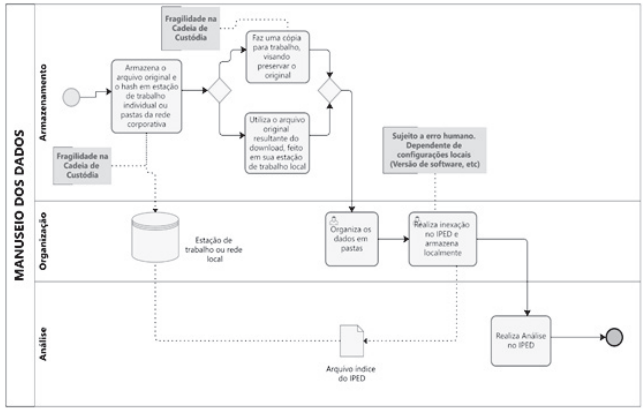

Figura 7. Modelagem – Manipulação dos dados
(Fonte: elaboração dos autores, 2023).

telemáticos. As questões foram elaboradas e respondidas por meio da plataforma Google, na ferramenta Google Forms. Esta avaliação preliminar não esgota o assunto e muito menos elimina um diagnóstico mais profundo e preciso; no entanto, as repostas foram bastante esclarecedoras, corroborando o direcionamento desta pesquisa. Os resultados apresentados no diagnóstico podem ser resumidos em três pontos principais e extremamente relevantes – armazenamento, organização (arquivamento digital) e velocidade da rede os quais detalhamos a seguir. Os resultados obtidos com a pesquisa reafirmaram a existência de problemas na gestão dos dados telemáticos e os efeitos danosos que podem trazer ao processo da persecução criminal.

INFRAESTRUTURA DE ARMAZENAMENTO

Ao realizar o download dos dados da empresa de tecnologia (após todo o rito legal e apropriado), o investigador precisa de espaço para armazenamento e dispositivos de

armazenamento adequados. As evidências digitais precisam ser mantidas o tempo necessário do processo criminal e pode levar até 3 anos dependendo do caso. A pesquisa diagnóstica preliminar apontou que os dados telemáticos ficam localizados em quase 58% no armazenamento local (computador ou estação de trabalho, HDs externos ou pendrives) e de cerca de 34% no armazenamento em rede (pastas de rede ou equivalente) existentes na instituição (Figura 8).

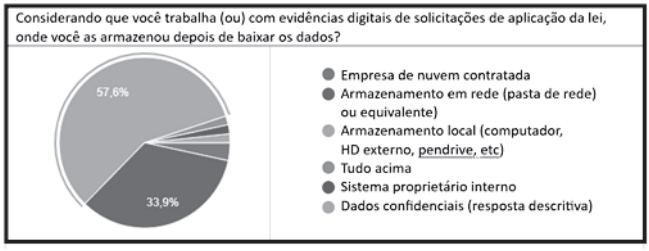

Figura 8. Principal armazenamento - dispositivos locais
(Fonte: elaboração dos autores, 2023).

Em relação a outros arquivos e evidencias de casos e trabalhos realizados que não são relacionados com requisições de dados telemáticos, o armazenamento preferido é o armazenamento em rede com 49% das respostas seguido pelo armazenamento local com 32% (Figura 9).

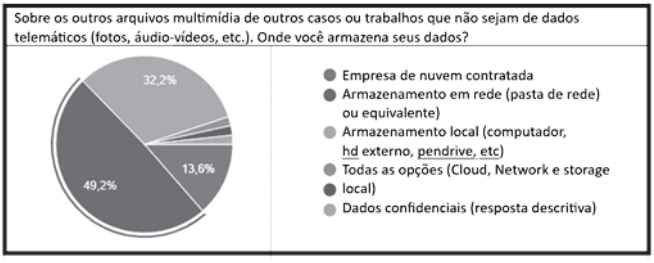

Figura 9. Armazenamento de outros dados
(Fonte: elaboração dos autores, 2023).

Em relação ao volume, cerca de 42% dos entrevistados informaram volume armazenado superior a 1Tb e 25% acima de 100 Gb (Figura 10).

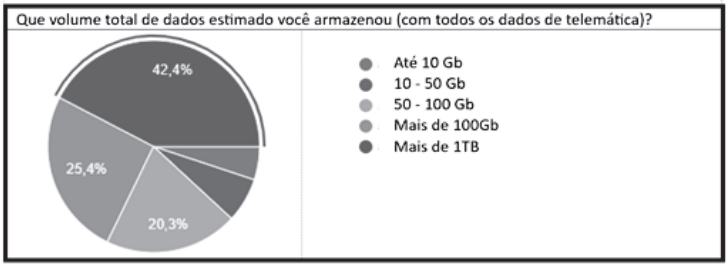

Figura 10. Volume armazenado - Superior a 1 Tb
(Fonte: elaboração dos autores, 2023).

De imediato, temos o cenário problema de armazenamento pulverizado em dispositivos locais individuais e dispersos em vários ambientes, tornando praticamente impossível a gestão e organização destes dados, além de alto risco de comprometimento da cadeia de custódia das evidências.

ORGANIZAÇÃO DOS ARQUIVOS

A pesquisa diagnóstica preliminar apontou para um percentual de cerca de 76% de uso de organização individual (método de arquivamento próprio), 18% no uso de arquivamento já existente e os demais sem nenhuma metodologia de arquivamento, deixando os arquivos nas pastas padrões do sistema - Meus Documentos (Figura 11).

Os arquivos armazenados precisam de um mínimo de padronização no arquivamento para uma posterior recuperação da informação. Caso cada investigador use sua organização (arquivamento digital) própria, é possível que

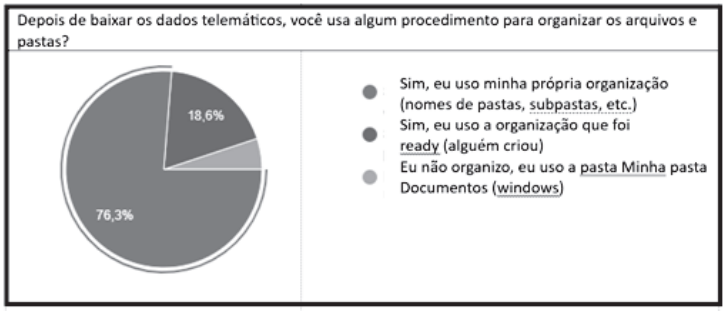

Figura 11. Principal meio de organização dos arquivos - Individual (Fonte: elaboração dos autores, 2023).

haja divergências numa busca local de informações, como duplicações, pastas e diretórios diferentes e principalmente em estações de trabalhos ou dispositivos de armazenamentos diferentes. Esse resultado nos direciona a um ambiente de dados completamente sem padronização e de difícil recuperação da informação.

VELOCIDADE INTERNA DA REDE

Embora exista uma robusta estrutura de rede na Polícia Federal, a demanda e o tráfego dos dados em rede nacional afetam diretamente a velocidade de download de forma diferente em todo o país, impactando no trabalho de obtenção (coleta) dos dados das empresas de tecnologia por meio desta rede. Não obstante, o risco de um download incompleto ou corrompido é possível e exigiria o reinício de todo o trabalho. A pesquisa diagnóstica preliminar apontou como causa da principal dificuldade em trabalhar com quebra de sigilo telemático são a velocidade de rede e o espaço de armazenamento com cerca 37% em ambas as respostas (Figura 12).

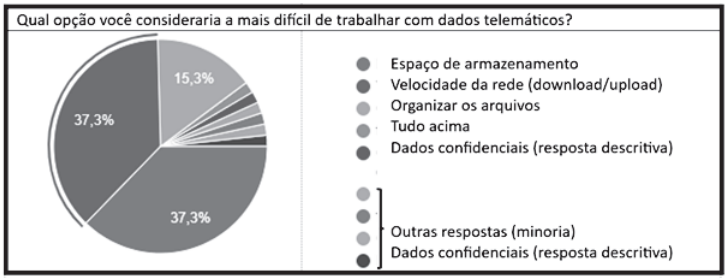

Figura 12. Maior dificuldade - Velocidade e Armazenamento (Fonte: elaboração dos autores, 2023).

Observamos em terceiro lugar, com cerca de 15%, a dificuldade com a organização (arquivamento digital), apontada como sendo a maior dificuldade dos investigadores.

CONSIDERAÇÕES FINAIS

Os resultados obtidos com a avaliação diagnóstica já permitem inferir algumas conclusões que corroboram com o cenário prático. Significando que, mesmo com uma rotina semelhante entre os diversos profissionais da investigação, cada um em seu grupo de trabalho irá executar a tarefa de forma parecida, porém não padronizada. Em outras palavras, a coleta e o armazenamento dos dados de quebra de sigilo telemático seguem processo não padronizado, no qual os arquivos seriam armazenados em locais diferentes e organizados de formas diferentes (Figura 13).

Diversos ambientes de investigação trabalham com suas próprias metodologias parecidas, mas não padronizadas. Uma solução plausível para este cenário seria a criação de uma ferramenta tecnológica, como uma plataforma Web, que servisse de interface para a aquisição, arquivamento digital, armazenamento dos dados e incluindo a gestão das interações com a evidência, padronizando o pré-processamento dos dados para

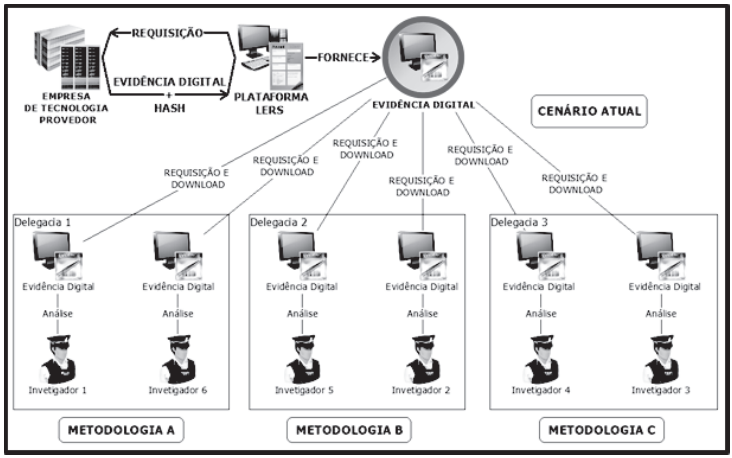

Figura 13. Procedimentos similares, mas não padronizados (Fonte: elaboração dos autores, 2023).

todos os usuários. Durante esta pesquisa, foram encontradas propostas de gestão e armazenamento de evidências digitais que podem ser plenamente aproveitadas para os problemas identificados. Essas propostas, encontradas na literatura científica, trariam grandes melhorias no ambiente de investigação policial com os dados de quebra de sigilo telemático.

MODELO SUGERIDO

Em uma situação automatizada por meio de uma plataforma web e integrada a uma API (*Application Programming Interface*, ou, em português, interface de programação de aplicação), os dados fornecidos por meio de ordem judicial, extraídos de forma forense pela empresa de tecnologia, poderiam ser enviados diretamente para a plataforma *Web*. Processo que preserva imediatamente a autenticidade dos arquivos, e ainda organiza os dados de forma preestabelecida pela plataforma, o armazenamento seria possivelmente distribuído e integrado na rede institucional do órgão, e a velocidade de download

seria melhorada com o download centralizado em um link de alta velocidade. A ferramenta elimina a necessidade das etapas de download, arquivamento digital e armazenamento, antes realizada manualmente pelo investigador e ainda trazendo um robusto controle nas interações com a evidência, padronizando o pré-processamento dos dados para todos os usuários (Figura 14).

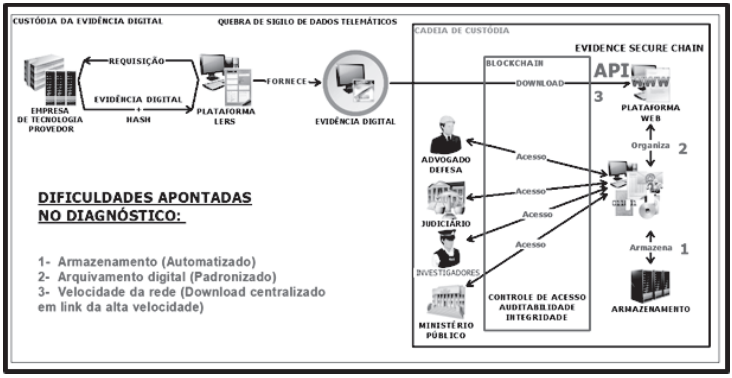

Figura 14. Ciclo de vida da evidência digital automatizado (Fonte: elaboração dos autores, 2023).

A proposta seria baseada numa plataforma *Web* (*frontend*) integrada a uma API, seria responsável por interagir com uma *Blockchain* para os registros das interações com as evidências digitais e o armazenamento. Nos diversos trabalhos já relacionados temos vários casos de utilização da tecnologia *Blockchain* para gestão e organização de evidências digitais envolvidas numa persecução criminal, embora não trate da aquisição direta das plataformas *LERS*.

A ideia proposta garantiria que, todo e qualquer procedimento envolvendo as transações com as evidências recebidas, por qualquer dos atores envolvidos, seria registrado em uma *Blockchain* e confirmado por consenso dentre os participantes permissionados (Polícia, Ministério

Público, Judiciário), garantiria ainda uma padronização no arquivamento dos dados e gestão da robusta cadeia de custódia de forma segura e imutável (Figura 15). Em outras palavras, seriam geridos pela plataforma a coleta, a organização (arquivamento digital) e o armazenamento, além do controle de todas as interações com a evidência digital, garantindo a autenticidade e integridade da cadeia de custódia e a lisura da investigação criminal. A escolha de uma *Blockchain* privada e permissionada é por óbvio uma necessidade de manter o sigilo dos dados pessoais envolvidos e o acesso somente aos atores autorizados no processo judicial, além do fato de que somente alguns participantes poderiam validar os blocos da rede pelo mecanismo de consenso da *Blockchain*. O armazenamento distribuído e integrado poderia facilitar a recuperação da informação bem como a análise dos diversos dados produzidos em múltiplas instâncias e épocas conforme a conveniência legal.

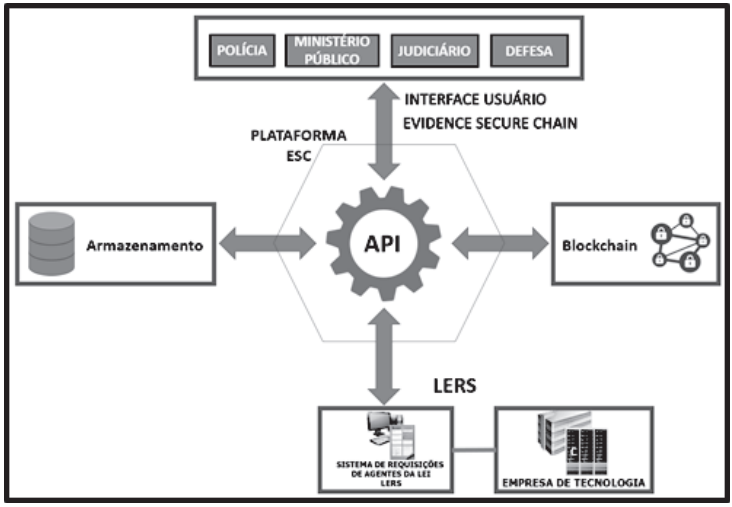

Figura 15. Solução proposta – API com plataforma Web + Blockchain + Armazenamento (Fonte: elaboração dos autores, 2023).

CONCLUSÕES

O universo da investigação policial exige do investigador uma grande capacidade cognitiva para compreender e reunir todos os elementos num único contexto. Quando esse trabalho passa a ter um grande e distinto volume de dados, a gestão e o armazenamento dos dados tornam-se mandatórios e o uso de ferramentas tecnológicas passa a ser primordial. Neste artigo, analisamos as possíveis implicações da falta de padronização, gestão e de armazenamento adequado no gerenciamento de evidências digitais oriundos de quebra de sigilo telemático na investigação criminal e aquisição junto as plataformas *LERS* das empresas de tecnologia.

A modelagem do processo estudado e avaliação diagnóstica mostraram claramente a necessidade de melhorar a aquisição dessas evidencias digitais. Em outra perspectiva, as etapas de coleta e armazenamento no pré-processamento podem ser comprometidas caso não tratadas adequadamente no ambiente da investigação policial, prejudicando o processo de descoberta de conhecimento e até invalidando a evidência criminal por deficiências na cadeia de custódia. Não somente isto, a gestão inadequada destes dados prejudicaria as etapas seguintes de uma mineração de dados ou uso de ferramentas de inteligência artificial.

A ideia proposta encontra aderência perfeita no cenário atual de inexistência de ferramenta tecnológica capaz de garantir a verificação da integridade, da autenticidade e da validade para todo o ciclo da evidência digital, gerada numa quebra de sigilo telemático nos portais *LERS*. E mais ainda, permitindo essa garantia a todos os atores envolvidos na persecução criminal, de forma ainda inédita no cenário nacional. E com aplicabilidade em todas as esferas da investigação criminal, sejam estaduais ou federais.

REFERÊNCIAS

AGARWAL, R, & DHAR, V. (2014). *Big Data, Data Science, and Analytics: The Opportunity and Challenge for IS Research*.

AHMAD, L. *et al*. (2020). *Blockchain-based chain of custody: towards real-time tamper-proof evidence management*. Em Proceedings of the 15th international conference on availability, reliability and security (pp. 1-8).

ANNE, V. P. K. *et al*. (2021). *Storing and Securing the Digital Evidence in the Process of Digital Forensics through Blockchain Technology*. Em Proceedings of the International Conference on Data Science, Machine Learning and Artificial Intelligence (pp. 272-276).

BARTH, F. J. *et al*. (2007). *Recuperação e mineração de informações para a área criminal*. Em ENIA VI-Encontro Nacional de Inteligência Artificial. Anais do XXVII Congresso da SBC (pp. 1292-1301).

BONOMI, S., CASINI, M., & CICCOTELLI, C. (2018). B-coc: A *Blockchain* -based chain of custody for evidences management in digital forensics. *arXiv preprint arXiv:1807.10359*.

BORKO, H. (1968). Ciência da Informação: o que é isto. *American Documentation, 19*(1), pp. 1-2.

BURRI, X. *et al*. (2020). Chronological independently verifiable electronic chain of custody ledger using blockchain technology. *Forensic Science International: Digital Investigation, 33*, p. 300976.

CHOPADE, M. *et al*. (2019). *Digital forensics: Maintaining chain of custody using Blockchain*. Em 2019 Third International conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC). IEEE (pp. 744-747).

DECRETO-LEI Nº 3.689, DE 3 DE OUTUBRO DE 1941, DO BRASIL. (1941). Código de Processo Penal, Presidência da República. Casa Civil - Subchefia para Assuntos Jurídicos.

FLORES, D., BRITO ROCCO, B. C., & SANTOS, H. M. (2016). *Cadeia de custódia para documentos arquivísticos digitais*.

GOPALAN, S. H. *et al*. (2019). Digital forensics using *Blockchain*. *International Journal of Recent Technology and Engineering,8*(2), pp. 182-184.

KHAN, A. A. *et al*. (2021). MF-ledger: blockchain hyperledger sawtooth-enabled novel and secure multimedia chain of custody forensic investigation architecture. *IEEE Access, 9*, pp. 103637-103650.

Li, M. *et al*. (2021). LEChain: A *Blockchain* -based lawful evidence management scheme for digital forensics. *Future Generation Computer Systems,115*, pp. 406-420.

Lone, A. H., & Mir, R. N. (2019). Forensic-chain: Blockchain based digital forensics chain of custody with PoC in Hyperledger Composer. *Digital investigation, 28*, pp. 44-55.

Martins, L., Emerich Lentz, V., & Barbosa, W. (2019). *Capitulo 4. Proposta de elementos conceituais para investigação criminal sob influência da Ciência da Informação. Aproximação entre a ciência da informação com a ciência policial*. SENAC.

Milagre, J. A., & Segundo, J.E. S. (2015). As contribuições da Ciência da Informação na perícia em informática no desafio envolvendo a análise de grandes volumes de dados - Big Data. *Informação & Tecnologia (ITEC), 2*(2), pp. 35-48.

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. *Decentralized Business Review*, p. 21260.

Olukoya, O. (2021). Distilling blockchain requirements for digital investigation platforms. *Journal of Information Security and Applications, 62*, p. 102969.

Petroni, B. C. A. *et al*. (2020). Smart contracts applied to a functional architecture for storage and maintenance of digital chain of custody using blockchain. *Forensic Science International: Digital Investigation, 34*, p. 300985.

Pastrana-Pardo, M. A., Ordóñez-Erazo, H. A., & Cobos-Lozada, C. A. (2022). Process Model Represented in BPMN for Guiding the Implementation of Software Development Practices in Very Small Companies Harmonizing DEVOPS and SCRUM. *Revista Facultad de Ingeniería, 31*(62).

Prado, G. (2014). *Prova penal e sistema de controles epistêmicos: a quebra da cadeia de custódia das provas obtidas por métodos ocultos*. São Paulo: Marcial Pons.

Saisse, R. (2017). Big Data Contra o Crime. *Revista Eletrônica Direito & TI, 1*(8), p. 16.

Saracevic, T. (1996). EMPTY, Ciência da informação: origem, evolução e relações. *Perspectivas em Ciência da Informação, 1*(1), p. 44. Recuperado 20 de abrilo de 2022, de http://hdl.handle.net/20.500.11959/brapci/37415

Saracevic, T. (1995). Interdisciplinary nature of information science. *Ciência da informação, 24*(1), pp. 36-41.

Souza, M., Almeida, F. G., & Souza, R. R. (2018). *O termo Big Data: quebra de paradigma dos n-V's*. Em Workshop de Informação, Dados e Tecnologia-WIDAT. Minas Gerais: Universidade Federal de Minas Gerais.

Tian, Z. *et al*. Block-DEF: A secure digital evidence framework using *Blockchain. Information Sciences, 491*, pp. 151-165, 2019.

Zanini, W. (2003). A arte de comunicação telemática: a interatividade no ciberespaço. *ARS (São Paulo),* 1, pp. 11-34.